

WHAT IS CLAIMED:

- 1 1. A method for establishing a trust relationship with a remote node,
2 comprising:
3 generating a local public value and a local private value on at least one
4 node;
5 receiving a public value from another node via an out-of-band mechanism;
6 and
7 generating a secret value using the local private value in combination with
8 the public value received from the other node.
- 1 2. A method according to Claim 1, wherein the method is performed on
2 both of a pair of nodes, and wherein further the secret values generated at both of the
3 nodes are symmetric.
- 1 3. A method according to Claim 2, wherein the generating a secret
2 value includes performing a Diffie-Hellman computation.
- 1 4. A method according to Claim 1, further comprising:
2 retaining the secret value locally;
3 protecting the secret value using the public value received from the other
4 node; and
5 transmitting the protected secret value to the other node via the out-of-band
6 mechanism.

1 5. A method according to Claim 4, wherein the generating a secret
2 value includes performing a Rivest-Shamir-Adleman (RSA) computation.

1 6. A method according to Claim 1, wherein the receiving of the public
2 value from the other node via an out-of-band mechanism includes receiving the public
3 value over an asynchronous connection.

1 7. A method according to Claim 1, wherein the receiving of the public
2 value from the other node via an out-of-band mechanism includes downloading the
3 public value from an external device.

1 8. A method according to Claim 7, wherein the external device is any
2 one of a personal digital assistant (PDA), flash memory, memory stick, barcode, smart
3 card, USB-compatible device, Bluetooth-compatible device, and infrared-compatible
4 device.

1 9. A computer-readable medium having one or more instructions
2 causing one or more processors to:
3 generate a local two-part code having a public code component and private
4 code component;
5 receive a public code component from another processor via a peripheral
6 device; and
7 generate a secret value using the local private code component and the
8 public code component received from the other processor.

1 10. A computer-readable medium according to Claim 9, wherein the one
2 or more instructions are executed on the other processor, and wherein further the secret
3 value is symmetrical to the secret value generated on the other processor.

1 11. A computer-readable medium according to Claim 9, wherein the one
2 or more instructions to generate a secret value includes one or more instructions to
3 perform a Diffie-Hellman computation.

1 12. A computer-readable medium according to Claim 9, further
2 comprising one or more instructions causing one or more processors to:
3 encode the secret value using the public code component received from the
4 other processor; and
5 transmit the encoded secret value to the other processor via the peripheral
6 device.

1 13. A computer-readable medium according to Claim 12, wherein the
2 one or more instructions to generate a secret value includes one or more instructions to
3 perform an RSA computation.

1 14. A computer-readable medium according to Claim 9, wherein the
2 peripheral device is asynchronously connected to the one or more processors.

1 15. A computer-readable medium according to Claim 9, wherein the one
2 or more instructions to receive the public code component from the other processor via

3 the peripheral device includes downloading the public code component from one of a
4 personal digital assistant (PDA), flash memory, memory stick, barcode, smart card, USB-
5 compatible device, Bluetooth-compatible device, and infrared-compatible device.

1 16. An apparatus, comprising:
2 a key generator to generate a local public/private key pair; and
3 a shared secret generator to receive a public key from another node via an
4 out-of-band connection and to generate a shared secret using the local private key and the
5 public key received from the other node.

1 17. An apparatus according to Claim 16, wherein the shared secret is
2 symmetrical to a shared secret generated on the other node using the local public key and
3 a private key corresponding to the other node.

1 18. An apparatus according to Claim 16, wherein the other node is a
2 server.

1 19. An apparatus according to Claim 16, wherein the shared secret
2 generator is to generate a shared secret by performing a Diffie-Hellman computation.

1 20. An apparatus according to Claim 16, further comprising an encoder
2 to encode the secret value using the public key received from the other node and to
3 transmit the encoded secret value to the other node via the out-of-band connection.

1 21. An apparatus according to Claim 20, wherein the shared secret
2 generator is to generate a shared secret by performing an RSA computation.

1 22. An apparatus according to Claim 16, wherein the out-of-band
2 connection includes any one of a personal digital assistant (PDA), flash memory, memory
3 stick, barcode, smart card, USB-compatible device, Bluetooth-compatible device, and
4 infrared-compatible device.

1 23. A protocol for establishing trust between two or more processing
2 nodes, comprising:
3 generating a public key and a private key on each of at least two nodes;
4 exchanging the public keys between the at least two nodes using an
5 asynchronous mechanism; and
6 calculating a secret to be shared on at least one of the two nodes.

1 24. A protocol according to Claim 23, wherein the calculating of the
2 secret to be shared includes performing a function using the public key from the other of
3 the two nodes and the private key.

1 25. A protocol according to Claim 24, wherein the calculating the secret
2 to be shared includes performing a Diffie-Hellman calculation.

1 26. A protocol according to Claim 24, wherein the secret to be shared is
2 symmetrical on the at least two nodes.

1 27. A protocol according to Claim 23, further comprising:
2 encoding the secret to be shared using the public key from the other of the
3 two nodes; and
4 transmitting the encoded secret to be shared to the other of the two nodes
5 via the asynchronous mechanism.

1 28. A protocol according to Claim 27, wherein the calculating the secret
2 to be shared includes performing an RSA calculation.

1 29. A protocol according to Claim 23, wherein the out-of-band
2 mechanism includes any one of a personal digital assistant (PDA), flash memory,
3 memory stick, barcode, smart card, USB-compatible device, Bluetooth-compatible
4 device, and infrared-compatible device.

1 30. An apparatus, comprising:
2 means for generating a local public/private key pair; and
3 means for receiving a public key from another node via an out-of-band
4 connection; and
5 means for generating a shared secret using the local private key and the
6 public key received from the other node.

1 31. An apparatus according to Claim 30, wherein the means for
2 generating a shared secret performs a Diffie-Hellman computation.

1 32. An apparatus according to Claim 30, further comprising means for
2 encoding the shared secret using the public key received from the other node.

1 33. An apparatus according to Claim 32, wherein the means for
2 generating a shared secret performs an RSA computation.

1 34. An apparatus according to Claim 30, wherein the out-of-band
2 connection includes any one of a personal digital assistant (PDA), flash memory, memory
3 stick, barcode, smart card, USB-compatible device, Bluetooth-compatible device, and
4 infrared-compatible device.